PHYSICAL SECURITY POLICY

City of Helena/Lewis and Clark County IT&S

Information Security Policy Manual

Version Control

Policy Code:	ITSEC010	Approved By:	IT&S Steering Committee 3/24/2021 IT Board 4/8/2021
Owner:	IT&S	Effective Date:	4/8/2021

Revision History

Date	Version	Created by	Description of change

Table of Contents

1. Purpose and Scope

The purpose of this policy is to establish the physical security requirements of sensitive information and City of Helena/Lewis and Clark County IT&S (IT&S) technology resources throughout all levels of operations.

Physical security is used to protect sensitive data and technology resources from potential threats including:

- Unauthorized use
- Theft
- Natural or man-made disaster
- General emergency

This document applies to all IT&S employees and information systems, as well as any visitors or contractors.

2. Roles and Responsibilities

IT&S is responsible for communicating the physical security requirements of this policy to all relevant stakeholders, as well as providing general guidance to departments and end users regarding physical security controls and best practices. Departments and end users are responsible for implementing physical security measures in compliance with the requirements of this policy to ensure office areas, workstations, output devices (e.g. Printers), and sensitive documents are appropriately secured.

The Security Officer ensures that the provisions of this policy are implemented at all facilities, and regularly reviews and updates the Physical Security Policy to ensure it is current and accurate. Additionally, the Security Officer will ensure the proper identification and reporting of suspected or actual breaches of physical security in accordance with the *Incident Response Policy*.

3. Facility Security Plan

IT&S will implement physical security measures to protect its information, technology resources, and the facilities in which they are housed. Such protections include adequate physical construction of facilities, security controls at physical entry points, as well as additional physical barriers.

3.1 Access Controls

IT&S will implement access controls to prevent unauthorized physical access, tampering, or theft of IT&S assets, including both IT resources and sensitive information. Access controls are required for IT&S offices and secure areas.

Examples of access controls include:

- Security staff
- Manual key locks
- Keypad locks

All of IT&S's facilities will include one or more locations that are inaccessible to the public, called Secure Areas. These secure areas must have doors and windows that are locked by default, as well as surveillance systems and alarms. Many of these secure areas will also have additional security controls.

Some Examples of Secure Areas include:

- Server rooms / data centers
- Back-up storage areas
- Employee offices

Access controls will be implemented to restrict, authorize, and monitor access to the IT&S facility and the identified secure areas during both business and non-business hours.

Devices or physical documents with sensitive information must be kept in secure office areas or locked storage areas within the IT&S facility. Backup media are also located in a secure off-site location, and media are exchanged weekly between the off-site storage location and IT&S Department.

3.2 Access Management

Access to City of Helena/Lewis and Clark Country office facilities and secure areas will be restricted based on job role. For example, only select employees will need access to facilities outside of normal business hours, and access to server rooms and IT&S storage will not be needed by most employees.

The Security Officer is responsible for communicating and coordinating approval, modifications, and termination of physical access in a accordance with the Access Control Policy. This also includes issuing and revoking alarm codes, keys, fobs, access badges, and other physical access credentials as needed. Facility keys and alarm codes will be tightly restricted and secured.

Employees will be required to use the facility key and/or fob that has been issued to them in order to gain access to the facility and secure areas. Lost or stolen keys or fobs must be reported immediately to Supervisors and/or the Security Officer. Steps will then be taken to immediately disable badges and/or change locks as needed. Alarm codes will be immediately changed in response to transfers or departures of employees who have knowledge of the codes, and in response to suspected compromise or other security incidents.

3.3 Visitor Access Validation

Access to the IT&S Office is restricted through a locked and secure door. During business hours, visitors must request access by pushing an intercom button. Pushing the button initiates a phone call to Helpdesk and allows the visitor and IT&S staff to interact. Helpdesk can then approve access by unlocking the door or deny entry.

Maintenance personnel must give IT&S prior notice before entering the property and may require supervision when working in secure areas (i.e. server room). Custodians and maintenance personnel may be required to sign a Nondisclosure Agreement if working in secure areas or locations that may allow access to sensitive information.

3.4 Contingency Operations

IT&S facilities and associated assets must be protected from external environmental threats such as natural disasters, fires, floods, etc. Such protections include the use of environmental controls that will mitigate environmental threats to equipment. All secure areas, such as data centers and server rooms, must reside within solid structures and be kept at an appropriate temperature for the equipment therein. These buildings and/or secure areas must also have appropriate fire and natural gas detection systems, as well as alarm and suppression systems. The following environmental controls may be implemented for effective environmental protection:

- Water and Smoke detectors
- Fire Extinguishers
- Temperature Control

- Fireproof Storage

In the event of an emergency or disaster, the Security Officer will need access to the main office, the back-up storage location, the data center, as well as the ability to contact any third party backup vendors.

For a more detailed contingency plan, consult the *Business Continuity Policy*.

3.5 Maintenance Records

IT&S requires that records of all security-related maintenance and repairs are kept. Repairs to hardware, walls, doors, locks and security instruments (cameras, alarms, etc.) should be recorded in a Maintenance Repair Log, or in the form of organized invoices. The Security Officer is responsible for collecting and updating this information.

4. Workstation Security

IT&S will enforce physical security standards for all workstations, fax machines, printers, etc. All workstations that have access to sensitive information must be kept in a secure area whenever possible. Monitors should face away from areas of public view and users should lock workstations when leaving them unattended. Devices will also be configured to activate automatic screen savers after inactivity. All print jobs containing sensitive information must be immediately retrieved from the printer tray to ensure only authorized personnel access the physical document.

IT&S will also maintain an inventory of workstations as per the Asset Management policy and will store unused workstations in a secure area.

While IT&S is responsible for communicating expectations for workstation security, individual departments and end users are ultimately responsible for implementing these requirements by taking reasonable steps to secure devices and ensure monitors are appropriately positioned as mandated by the Acceptable Use Policy. Department heads are encouraged to perform periodic spot checks to ensure workstations and output devices are appropriately secured, and take steps to address any deficiencies by requesting privacy screens or further training and assistance from IT&S as needed. In the event of a security incident involving a workstation or output device, IT&S will follow up with the impacted end user and/or department to review the physical security measures in place and determine corrective actions to prevent reoccurrence. Users should refer to the Clear Desk and Clear Screen section of the Acceptable Use Policy for the physical security requirements that all users are expected to adhere to for securing devices and sensitive documents.

5. Policy Maintenance and Management

The owner of this document must evaluate and perform any necessary updates to this document at least once per year. The owner may delegate tasks related to this policy as appropriate.

- The Security Officer will adhere to the continual validation, review, and updating of this policy.

- When evaluating this policy, the number of instances of unauthorized access to IT&S facilities and secure areas will be considered.

6. References

NIST Cybersecurity Framework References

- PR.AC – Access Control
- PR.AT – Awareness and Training

- PR.DS – Data Security
- PR.IP – Information Protection Processes and Procedures
- PR.MA - Maintenance
- DE.CM – Security Continuous Monitoring

Policy References

- Business Continuity Plan
- Access Control Policy
- Asset Management Policy
- Incident Response Policy